UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/592,322	06/13/2000	Slawomir K. Ilnicki	10992668-1	7389

22879 7590 11/03/2005

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 11/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/592,322	ILNICKI ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 January 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22 and 24-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22,24-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the appeal brief filed on January 5, 2005, PROSECUTION IS HEREBY REOPENED. A new grounds of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

Response to Amendment

2. The proposed amendment filed on September 31, 2004 has been entered by the examiner canceling claim 23.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 11,14,17,19, and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by MacKenzie et al, U.S. Patent 6,757,825.

As per claim 11, MacKenzie et al discloses of a method of securely transferring data between an application server and an agent of the application server through a non-secure environment having a web-server and the agent, the method comprising a user accessing the web-server to download the agent therefrom; wherein the agent includes a public key of the application server, the agent deriving a shared session key with the application server by using the public key of the application server, the shared session key for use in encrypting and decrypting data to be transferred between the agent and the application server; the application server establishing a connection to the web-server; and the agent contacting the web server by using a first protocol to send data encrypted by the session key to the application server over the connection between the web-server and the application server (col. 3, lines 5-17 and col. 8, lines 12-27).

As per claim 14, it is disclosed by MacKenzie et al that the first protocol is one of HTTP and HTTP/SSL (col. 3, lines 5-23).

As per claim 17, MacKenzie et al teaches of a secure data transfer system for establishing an end-to-end secure connection between an agent and an application server behind a firewall through a nonsecure node comprising a web-server residing in the non-secure node, the web-server having the agent that includes a public key of the application server; a browser in communication with the web-server for downloading the agent from the web-server; a secure transfer module residing in the non-secure node; and an application server in a secure zone for initiating a connection to the web server via the secure transfer module port (col. 1, lines 37-43, col. 3, lines 5-17, and col. 8, lines 12-27).

As per claim 19, MacKenzie et al discloses that the non-secure node is a web server node (col. 3, lines 5-23).

As per claim 21, MacKenzie et al teaches of transferring data between the agent and the web server via an unsecure communication link (col. 1, lines 37-43 and col. 3, lines 5-23).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-10,12,13,15,16,18,20,22 and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over MacKenzie et al, U.S. Patent 6,757,825.

As per claim 1, it is disclosed by method for securely transferring data between an agent and an application server through a non-secure node comprising establishing a session key between the agent and the application server by utilizing a public key of the application server; wherein the public key of the application server is embedded in the agent to enable the agent to derive the session key; and establishing an end-to-end secure connection between the agent and the application server by using the session key and by establishing a communication link between the application server and the non -secure node (col. 3, lines 5-17 and col. 8, lines 12-27). The teachings of MacKenzie et al are silent in disclosing of establishing a communication link between the application server and the non-secure node using a relay module. The examiner asserts that it is obvious to make use of a router that acts as a relay module to connection two remote entities. It is obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply use of a router. Routers are notoriously well known to connect many computers through a mesh of possible connections in order to facilitate message delivery by forwarding messages to the correct destination by using the most efficient route that is available. It is obvious that the teachings of MacKenzie et al use routers so that the encrypted communications are corrected forwarded to the proper destination.

As per claims 2 and 18, MacKenzie et al teaches of establishing a communication link between the application server and, the non-secure node by using a relay module comprises dynamically instantiating, by the application server, the relay module having a first port for communicating with the application server and a second port for communicating with the agent, the relay module listening, on a first predetermined port number on the first port and a second predetermined port number on the second port; and the application server connecting to the first port of the relay module to establish a connection therewith (col. 1, lines 37-43, col. 3, lines 5-17, and col. 8, lines 12-27). Please refer above for the examiner's interpretation of the relay module being a router and the applied obviousness rejection with the supplied motivation.

As per claim 3, MacKenzie et al discloses of establishing a communication link between the application server and the agent through a relay module further comprises pushing data encrypted by the established session key from the agent to the application server over the end-to-end secure connection (col. 8, lines 12-27). Please refer above for the examiner's interpretation of the relay module being a router and the applied obviousness rejection with the supplied motivation.

As per claim 4, it is taught by MacKenzie et al of establishing a communication link between the application server and the agent through a relay module further comprises pulling data encrypted by the session key from the application server over the end-to-end secure connection to the agent (col. 8, lines 12-27). Please refer above

for the examiner's interpretation of the relay module being a router and the applied obviousness rejection with the supplied motivation.

As per claim 5, it is disclosed by MacKenzie of establishing a session key between the agent and the application server by utilizing a public key of the application server further comprises establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent there between (col. 3, lines 5-17 and col. 8, lines 12-27).

As per claim 6, MacKenzie et al teaches of establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent there between comprises encrypting the shared secret key with the public key of the application server to generate an encrypted shared key; sending the encrypted shared secret key to the application server; and decrypting the shared secret key with the private key of the application server (col. 3, lines 5-17 and col. 4, lines 25-34).

As per claim 7, MacKenzie et al discloses of establishing a shared secret key between the application server and the agent utilizes a key transfer protocol (col. 3, lines 5-24).

As per claim 8, the teachings of MacKenzie et al recite wherein the key transfer protocol is the Rivest, Shamir, Adleman (RSA) public key algorithm (col. 3, lines 51-58).

As per claim 9, MacKenzie et al discloses of establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent there between utilizes a key agreement protocol (col. 8, lines 12-27).

As per claim 10, MacKenzie et al teaches that the key agreement protocol is the DiffieHellman (DH) public key algorithm (col. 8, lines 12-27).

As per claim 12, MacKenzie et al discloses that the application server establishing a connection to the web server further comprises the application server sending a URL to the web-server, the URL specifying a first predetermined port for communication with the web-server; the application server connecting to a first predetermined port; and the application server reading data through the connection on the first predetermined port (col. 1, lines 37-43, col. 3, lines 5-17, and col. 8, lines 12-27). The teachings of MacKenzie et al are silent in disclosing of establishing a communication link between the application server and the non-secure node using a relay module. The examiner asserts that it is obvious to make use of a router that acts as a relay module to connection two remote entities. It is obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply use of a router. Routers are notoriously well known to connect many computers through a mesh of possible connections in order to facilitate message delivery by forwarding messages to the correct destination by using the most efficient route that is available. It is obvious that the teachings of MacKenzie et al use routers so that the encrypted communications are corrected forwarded to the proper destination.

As per claim 13, it is taught by MacKenzie et al that the agent contacting the web-server by using a first protocol to send data encrypted by the session key to the application server over the connection between the web server and the application server further comprises the agent encrypting the session key with the public key of the

application server; the agent collecting data; the agent encrypting the collected data with the session key; sending the encrypted session key and encrypted measured data to the application server by using a forwarding module that connects to a second predetermined port of the relay module (col. 3, lines 5-17, and col. 8, lines 12-27), please refer above for the examiner's interpretation of the relay module being a router and the applied obviousness rejection with the supplied motivation.

As per claim 15, MacKenzie et al discloses of a secure data transfer system for connecting a non-secure node to an application server behind a firewall comprising a web-server in the non-secure node that is configured by the application server to have a first port for listening for a connection from the application server; wherein the application server connects to the first port and reads data from the first port (col. 1, lines 37-43, col. 3, lines 5-17, and col. 8, lines 12-27). The teachings of MacKenzie et al are silent in disclosing of establishing a communication link between the application server and the non-secure node using a relay module. The examiner asserts that it is obvious to make use of a router that acts as a relay module to connection two remote entities. It is obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply use of a router. Routers are notoriously well known to connect many computers through a mesh of possible connections in order to facilitate message delivery by forwarding messages to the correct destination by using the most efficient route that is available. It is obvious that the teachings of MacKenzie et al use routers so that the encrypted communications are corrected forwarded to the proper destination.

As per claim 16, MacKenzie et al discloses wherein the relay does not initiate the connection with the application server but waits for the application server to establish the connection (col. 1, lines 37-43, col. 3, lines 5-17, and col. 8, lines 12-27), please refer above for the examiner's interpretation of the relay module being a router and the applied obviousness rejection with the supplied motivation.

As per claim 20, MacKenzie et al teaches of transferring data between the agent and the relay module via an unsecure communication link (col. 1, lines 37-43 and col. 3, lines 5-23), please refer above for the examiner's interpretation of the relay module being a router and the applied obviousness rejection with the supplied motivation.

As per claim 22, it is disclosed by MacKenzie et al of a method, comprising embedding in code of an agent a public key of an application server that is behind a firewall. downloading the code of the agent and the public key into a browser, verifying the agent to authenticate the public key of the application server, establishing a communication link with the application server that is in a non-secure environment and with the browser, and securely transferring data from the browser to the application server without requiring a trusted intermediate party (col. 1, lines 37-43, col. 3, lines 5-17, and col. 8, lines 12-27). The teachings of MacKenzie et al are silent in disclosing of establishing a communication link between the application server and the non-secure node using a relay module. The examiner asserts that it is obvious to make use of a router that acts as a relay module to connection two remote entities. It is obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply use of a router. Routers are notoriously well known to connect many computers

through a mesh of possible connections in order to facilitate message delivery by forwarding messages to the correct destination by using the most efficient route that is available. It is obvious that the teachings of MacKenzie et al use routers so that the encrypted communications are corrected forwarded to the proper destination.

As per claim 24. MacKenzie et al teaches of comprising collecting data with the agent (col. 3, lines 5-17).

As per claim 25, it is taught by MacKenzie et al of collecting data with the agent further comprises measuring time required to load data into the browser (col. 1, lines 37-43 and col. 3, lines 5-23).

As per claim 26, MacKenzie et al discloses that the communication link between the browser and the relay module is an unsecure communication link (col. 1, lines 37-43 and col. 3, lines 5-23), please refer above for the examiner's interpretation of the relay module being a router and the applied obviousness rejection with the supplied motivation.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
Primary Examiner
AU 2131

CR

October 28, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100